

# A FINITARY HASSE PRINCIPLE FOR DIAGONAL CURVES

JEAN BOURGAIN AND MICHAEL LARSEN

**ABSTRACT.** We prove a Hasse principle for solving equations of the form  $ax + by + cz = 0$  where  $x, y, z$  belong to a given finite index subgroup of  $\mathbb{Q}^\times$ . From this we deduce a Hasse principle for diagonal curves over subfields of  $\bar{\mathbb{Q}}$  with finitely generated Galois group.

## 1. INTRODUCTION

Let  $a, b, c$  be non-zero rational numbers and  $n \geq 2$  an integer. Let  $X$  denote the projective curve  $ax^n + by^n + cz^n = 0$ . For  $n = 2$ , the following are equivalent:

- (1)  $X(\mathbb{Q}_p) \neq \emptyset$  for all  $p$  and  $X(\mathbb{R}) \neq \emptyset$ .
- (2)  $X(\mathbb{Q}) \neq \emptyset$ .
- (3)  $X(\mathbb{Q})$  is infinite.

The equivalence of (1) and (2) is the Hasse-Minkowski theorem for conics over  $\mathbb{Q}$ , while the equivalence of (2) and (3) follows from stereographic projection. For  $n > 2$ , neither equivalence holds in general. Already for  $n = 3$ , the Tate-Shafarevich group gives an obstruction to  $(1) \Rightarrow (2)$ ; for instance, Selmer showed that  $3x^3 + 4y^3 + 5z^3 = 0$  has local solutions for all places of  $\mathbb{Q}$  but no global solution [7, p. 8]. For  $a = b = -c = 1$ , Fermat's Last Theorem shows that (2) does not imply (3) for any  $n \geq 3$ .

We fix once and for all an algebraic closure  $\bar{\mathbb{Q}}$  of  $\mathbb{Q}$ . We can view elements of  $X(\mathbb{Q})$  as elements of  $X(\bar{\mathbb{Q}})$  which are invariant under the action of  $G_{\mathbb{Q}} := \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ . As  $G_{\mathbb{Q}}$  is not finitely generated, this can be regarded as an infinitary condition. It turns out that if we replace invariance under  $G_{\mathbb{Q}}$  by any finite collection of invariance conditions, the equivalence of conditions (1)–(3) as above holds for all  $n$  and all  $a, b, c$ .

Let  $\Sigma \subset G_{\mathbb{Q}}$  be any finite subset. Let

$$K_{\Sigma} := \{x \in \bar{\mathbb{Q}} \mid \sigma(x) = x \ \forall \sigma \in \Sigma\}$$

denote the field of invariants of the closed subgroup  $\langle \Sigma \rangle$  generated by  $\Sigma$ . A subfield  $K$  of  $\bar{\mathbb{Q}}$  is of this form if and only if its absolute Galois group  $G_K$  is (topologically) finitely generated. We prove the following theorem:

---

*Date:* April 11, 2014.

Jean Bourgain thanks the Berkeley math department for its hospitality. Michael Larsen thanks the MSRI for its hospitality and also wants to acknowledge support from NSF grant DMS-1101424 and the Simons Foundation.

**Theorem 1.** *Given  $a, b, c \in \mathbb{Q}^\times$  and  $n$  a positive integer, the following conditions on the projective curve  $X : ax^n + by^n + cz^n = 0$  are equivalent:*

- (1)  $X(\mathbb{Q}_p) \neq \emptyset$  for all  $p$  and  $X(\mathbb{R}) \neq \emptyset$ .
- (2)  $X(K) \neq \emptyset$  for all  $K \subset \bar{\mathbb{Q}}$  with  $G_K$  finitely generated.
- (3)  $|X(K)| = \infty$  for all  $K \subset \bar{\mathbb{Q}}$  with  $G_K$  finitely generated.

One can prove that (2) implies (3) in greater generality:

**Theorem 2.** *If  $K$  is a field in characteristic zero such that  $G_K$  is finitely generated, then  $X(K)$  non-empty implies  $|X(K)| = \infty$ .*

The proof of Theorem 2 is purely combinatorial, following the strategy of [4].

The proof that (1) implies (2) is more difficult and depends on the following Hasse principle, unusual in that we need to consider finite combinations of local conditions:

**Theorem 3.** *Let  $G$  denote a finite index subgroup of  $\mathbb{Q}^\times$ , and let  $a, b, c$  belong to  $\mathbb{Q}^\times$ . For every set  $S$  of places of  $\mathbb{Q}$ , we define  $\mathbb{Q}_S := \prod_{v \in S} \mathbb{Q}_v$  and let  $G_S$  denote the closure of  $G$  in  $\mathbb{Q}_S^\times$ . Then*

$$(1) \quad ax + by + cz = 0$$

*has a solution for  $x, y, z \in G$  if and only if the same equation has a solution in  $G_S$  for all finite  $S$ .*

It is a striking fact that it does not suffice to check solvability in  $G_S$  for singleton sets  $S = \{v\}$ —see Proposition 9 below. We remark also that solving (1) in  $G$  is equivalent to solving it in any coset of  $G$ . Richard Rado [9] considered which systems of homogeneous linear equations have the property that for every finite partition of  $\mathbb{N}$ , the system can be solved with all variables belonging to a single part of the partition. In the case of a single equation (1), the system satisfies this property if and only if  $a + b = 0$ ,  $b + c = 0$ ,  $c + a = 0$ , or  $a + b + c = 0$ . In these special cases, therefore, Theorem 3 follows directly from Rado's theorem. This corresponds to the fact that Theorem 2 can be deduced from Ramsey theory, while the general case of Theorem 1 requires the circle method.

## 2. THE CIRCLE METHOD AND MULTIPLICATIVE FUNCTIONS ON $\mathbb{Q}$

In this section, we apply the circle method to prove Theorem 3. We begin with some preliminary lemmas.

We fix a finite index subgroup  $G \subset \mathbb{Q}^\times$  and non-zero  $a, b, c \in \mathbb{Q}$  such that  $ax + by + cz = 0$  has a solution in  $G_S$  for all finite sets  $S$  of places of  $\mathbb{Q}$ . We can freely replace  $a$ ,  $b$ , or  $c$  by any element in its  $G$ -coset, and we are free to multiply all three of them by a common non-zero rational number.

**Lemma 4.** *For all integers  $D > 0$ , there exist elements  $x, y, z \in G$  and  $w \in \mathbb{Q}^\times$  such that  $a' := wax$ ,  $b' := wby$ ,  $c' := wcz$  satisfy the following properties:*

- (a)  $\min(a', b', c') < 0$ ,

- (b)  $\max(a', b', c') > 0$ ,
- (c)  $a' + b' + c' \equiv 0 \pmod{D}$ ,
- (d)  $a', b'$  and  $c'$  are pairwise relatively prime,
- (e)  $a', b', c' \in \mathbb{Z}$ ,
- (f)  $a'b'c'$  is even.

*Proof.* The proof consists of a series of steps in which we replace  $a$ ,  $b$ , and  $c$  by  $wax$ ,  $wby$ , and  $wcz$  respectively, with the goal that at the end of the process, the resulting triple  $a, b, c$  satisfies properties (a)–(f).

Let  $\mathbb{P}$  denote the set of all prime numbers and  $\mathbb{P}_0$  the set of prime divisors of  $D$ . Let  $Q := \mathbb{Q}^\times / G$ , and define

$$\phi = (\phi_1, \phi_2): \mathbb{P} \setminus \mathbb{P}_0 \rightarrow Q \times (\mathbb{Z}/D\mathbb{Z})^\times,$$

where  $\phi_1$  denotes the restriction of the quotient map  $\mathbb{Q}^\times \rightarrow Q$  to  $\mathbb{P} \setminus \mathbb{P}_0$  and  $\phi_2$  denotes the restriction of  $\mathbb{Z} \rightarrow \mathbb{Z}/D\mathbb{Z}$  to  $\mathbb{P} \setminus \mathbb{P}_0$ . Let  $S$  be the union of all finite subsets of the form  $\mathbb{P} \cup \{\infty\} \setminus \phi^{-1}(Q')$  where  $Q'$  is a subgroup of  $Q \times (\mathbb{Z}/D\mathbb{Z})^\times$ . Thus  $S$  is finite, and if  $p \notin S$  and  $M$  is a given integer, then there exists a product  $m$  of primes  $> M$  such that  $\phi(pm) = 1$ .

By hypothesis, equation (1) has a solution  $(x_S, y_S, z_S)$  in  $G_S$ . Let  $x_v$  denote the  $v$ -component of  $x_S$  for  $v \in S$  and likewise for  $y_v, z_v$ . As  $ax_\infty + by_\infty + cz_\infty = 0$ , it follows that replacing  $a, b, c$  by  $ax, by, cz$ , where  $x, y, z$  are sufficiently close to  $x_\infty, y_\infty, z_\infty$ , the resulting triple satisfies properties (a) and (b).

Choose  $k$  to be a positive integer larger than

$$\max_{p \in S} \max(v_p(x_p), v_p(y_p), v_p(z_p)) + v_p(D)$$

and choose  $x, y, z \in G$  such that for all  $p \in S \setminus \{\infty\}$ ,

$$v_p(x_p - x), v_p(y_p - y), v_p(z_p - z) > k,$$

and  $ax, by$ , and  $cz$  are neither all positive nor all negative. Multiplying each of these by

$$w := \prod_{p \in S} p^{-\min(v_p(ax), v_p(by), v_p(cz))},$$

we obtain  $wax, wby, wcz$  which add to 0 (mod  $D$ ) and to zero (mod  $p$ ) for each  $p \in S$ . Moreover, for each  $p$ , all three belong to  $\mathbb{Z}_p^\times$ ; as they sum to zero (mod  $p$ ), at least one of the three belongs to  $\mathbb{Z}_p^\times$ ; as they sum to zero (mod  $p$ ), at least two are units. Replacing  $a, b, c$  by  $wax, wby, wcz$ , the resulting triple now satisfies properties (a)–(c), and at most one of  $v_p(a), v_p(b), v_p(c)$  is positive for  $p \in S$ .

If  $a, b$ , or  $c$  fails to be  $p$ -integral for some  $p \notin S$ , by definition of  $S$ , there exists  $m \in \mathbb{N}$  such that  $pm \in G$ ,  $pm \equiv 1 \pmod{D}$ , and all prime factors of  $m$  are as large as we may wish. In particular, we may assume that for each prime factor  $q$  of  $m$ ,  $q \neq p$ ,  $q \notin S$ , and  $v_q(a) = v_q(b) = v_q(c) = 0$ . Multiplying by  $pm$  eliminates a factor of  $p$  from the denominator of the desired element,  $a$ ,  $b$ , or  $c$ , without changing the residue class (mod  $D$ ) or the sign of the given element or introducing a common prime factor of any two elements of the set. Continuing this process as long as necessary, we can assume that

the resulting elements satisfy (a)–(e). If  $a$ ,  $b$ , and  $c$  are all odd, then  $D$  is odd as well, so  $2^k \equiv 1 \pmod{D}$  for some positive integer  $k$  divisible by  $|Q|$ ; replacing  $a$  by  $2^k a$ , we obtain a new triple  $a, b, c$  satisfying properties (a)–(f).  $\square$

**Lemma 5.** *Let  $D$  be a positive integer. Let  $a, b, c$  be integers satisfying conditions (a)–(f). There exists a constant  $\epsilon > 0$  and for every prime  $p$  a constant  $d_p > \max(1, 1 - 3/p)$  such that for every finite set  $S$  of primes not dividing  $D$ , the number of solutions of (1) in  $x, y, z \in (1 + D\mathbb{Z}) \cap [0, N]$  such that  $xyz$  is not divisible by any prime in  $S$  is at least*

$$N^2 \epsilon \prod_{p \in S} d_p$$

for all  $N$  sufficiently large.

*Proof.* By conditions (a)–(c), the intersection of  $ax + by + cz = 0$  with the cube  $[0, N]^3$  is a non-trivial polygonal region which up to homothety is independent of  $N$ . The intersection of  $ax + by + cz = 0$  with  $(1 + D\mathbb{Z})^3$  is the translate of a 2-dimensional lattice. If  $\Lambda$  is a lattice and  $R$  is a polygonal region, then

$$(2) \quad |\Lambda \cap (v + tR)| = \frac{\text{Area}(R)}{\text{Coarea}(\Lambda)} t^2 + O(t).$$

Thus, the number of solutions of (1) in  $x, y, z \in (1 + D\mathbb{Z}) \cap [0, N]$  is of the form  $AN^2 + O(N)$ . By condition (d), for each  $p \in S$ , the conditions  $p|x$ ,  $p|y$ , and  $p|z$  each define a sublattice of  $\Lambda$  of index  $p$ , so the subset  $\Lambda_p$  of  $\Lambda$  satisfying the condition  $p \nmid xyz$  is the union of  $p^2 \alpha_p$  cosets of  $p\Lambda$ , where  $\alpha_p > 1 - 3/p$ . By condition (f),  $\alpha_2 > 0$  if  $2 \in S$ .

Thus,  $\bigcap_{p \in S} \Lambda_p$  is the union of  $\prod_{p \in S} p^2 \alpha_p$  cosets of  $(\prod_{p \in S} p)\Lambda$ . The lemma now follows from (2).  $\square$

Let  $X$ ,  $Y$ , and  $Z$  be finite sets of integers. The number of solutions of (1) with  $x \in X$ ,  $y \in Y$ , and  $z \in Z$  can be written

$$(3) \quad \int_0^1 \sum_{x \in X} e(axy) \sum_{y \in Y} e(byt) \sum_{z \in Z} e(czt) dt$$

where  $e(t) := e^{2\pi i t}$ .

**Lemma 6.** *If  $|\alpha_x| = |\beta_y| = |\gamma_z| = 1$  for all  $x, y, z$ , then*

$$\begin{aligned} & \left| \int_0^1 \sum_{x \in X} \alpha_x e(axy) \sum_{y \in Y} \beta_y e(byt) \sum_{z \in Z} \gamma_z e(czt) dt \right| \\ & \leq \sup_t \left| \sum_{x \in X} \alpha_x e(axy) \right| |Y|^{1/2} |Z|^{1/2}. \end{aligned}$$

*Proof.* By Hölder and Cauchy-Schwartz,

$$\begin{aligned}
 & \left| \int_0^1 \sum_{x \in X} \alpha_x e(axy) \sum_{y \in Y} \beta_y e(byt) \sum_{z \in Z} \gamma_z e(czt) \right| \\
 & \leq \left\| \sum_{x \in X} \alpha_x e(axy) \right\|_\infty \left\| \sum_{y \in Y} \beta_y e(byt) \right\|_2 \left\| \sum_{z \in Z} \gamma_z e(czt) \right\|_2 \\
 & = \sup_{t \in [0,1]} \left| \sum_{x \in X} \alpha_x e(axy) \right| |Y|^{1/2} |Z|^{1/2}.
 \end{aligned}$$

□

**Corollary 7.** *If  $\delta > 0$ ,  $X' \subset X$  has at least  $(1 - \delta)|X|$  elements, and  $|\alpha_x| = |\beta_x| = |\gamma_x| = 1$  for all  $x \in X$ , then*

$$\begin{aligned}
 & \left| \int_0^1 \sum_{x \in X} \alpha_x e(axy) \sum_{y \in X} \beta_y e(byt) \sum_{z \in X} \gamma_z e(czt) dt \right. \\
 & \quad \left. - \int_0^1 \sum_{x \in X'} \alpha_x e(axy) \sum_{y \in X'} \beta_y e(byt) \sum_{z \in X'} \gamma_z e(czt) dt \right| \leq 3\delta |X|^2.
 \end{aligned}$$

Regarding the characters  $f \in Q^*$  as functions on  $Q^\times$  and therefore on  $X$ , we can write

$$(4) \quad \sum_{x \in X \cap G} e(axy) = \frac{1}{|Q|} \sum_{f \in Q^*} \sum_{x \in X} f(x) e(axy),$$

and likewise for  $\sum_{y \in X \cap G} e(byt)$  and  $\sum_{z \in X \cap G} e(czt)$ .

Every complex character  $\chi: Q^\times/G \rightarrow U(1)$  defines a homomorphism  $Q^\times \rightarrow U(1)$  and hence a strictly multiplicative function on  $\mathbb{N}$ . For each such function  $f$  there is at most one pair  $(\psi, t)$  consisting of a primitive Dirichlet character  $\psi$  and a real number  $t$  such that

$$(5) \quad \sum_p \frac{1 - \operatorname{Re}(f(p)\bar{\psi}(p)p^{-it})}{p} < \infty,$$

where the sum is taken over rational primes. Following terminology of Granville and Soundararajan [2], we will say that  $f$  is *pretentious* if such a pair exists.

If  $f$  takes values in a finite subgroup of  $U(1)$  (as in our case, where  $f$  arises from a homomorphism  $Q \rightarrow U(1)$ ), and if  $(\psi, t)$  satisfies (5), then  $t = 0$ . By a theorem of Halász [10, III.4 Theorem 4], for any multiplicative function  $f$  which takes values in the unit disk,

$$(6) \quad \sum_{n=1}^N f(n) = o(N)$$

unless  $f$  satisfies (5) for some  $t$  with  $\psi = 1$ . In our setting, this means (6) holds unless  $f(p) = 1$  outside a set  $\mathbb{P}_f$  of primes with

$$\sum_{p \in \mathbb{P}_f} \frac{1}{p} < \infty.$$

We denote by  $Q_{\text{pre}}^*$  the set of pretentious elements of  $Q^*$ . For each  $f \in Q_{\text{pre}}^*$  there exists a unique primitive Dirichlet character  $\psi$  such that  $f$  satisfies (5) with  $t = 0$ . We define  $\mathbb{P}_G$  to be the union of all the sets  $\mathbb{P}_{f\psi^{-1}}$  where  $f \in Q_{\text{pre}}^*$  and  $\psi$  is the primitive character associated to  $f$ . Again,

$$\sum_{p \in \mathbb{P}_G} \frac{1}{p} < \infty.$$

We define  $D := D_G$  to be the least common multiple of the conductors of all characters  $\psi$  associated with  $f \in Q_{\text{pre}}^*$ .

For  $h: \mathbb{N} \rightarrow \mathbb{C}$ ,  $\alpha \in \mathbb{R}$ , and  $n \in \mathbb{N}$ , we define

$$S_{h,n}(\alpha) := \sum_{x=1}^n e(\alpha x) h(x).$$

**Lemma 8.** *Let  $f: \mathbb{N} \rightarrow \mathbb{C}$  be the restriction of a homomorphism  $\mathbb{Q}^\times \rightarrow U(1)$  with finite image,  $g: \mathbb{Z} \rightarrow \mathbb{C}$  a periodic function, and  $\alpha \in \mathbb{R}$ . If  $f$  is not pretentious, then*

$$S_{fg,n}(\alpha) = o(n).$$

*Proof.* We claim that for all  $\epsilon > 0$ , there exists  $m$  such that for all  $n$  and all fractions  $\beta = r/s$  in lowest terms with  $m < s < n/m$ , we have

$$(7) \quad |S_{fg,n}(\beta)| \leq \epsilon n.$$

Indeed, if  $g(x)$  is periodic with period  $D$ , it can be written as a linear combination of  $e(\gamma x)$ ,  $\gamma \in D^{-1}\mathbb{Z}$ . The denominator of  $\beta + \gamma$ , written as a fraction in lowest terms, lies in  $(m/D, Dn/m)$ . By [8, Theorem 1], this implies (7) if  $m/D$  is sufficiently large.

If  $\beta = r/s$  with  $s \leq m$ , then  $S_{fg,\beta}$  is a linear combination of sums of the form  $S_{f,\beta+\gamma}$ , where there are only finitely many possibilities for  $\beta + \gamma \pmod{1}$ . For each possibility,  $e((\beta + \gamma)x)$  is periodic of some period  $k$  and can therefore be written as a linear combination of (not necessarily primitive)  $(\text{mod } k)$  Dirichlet characters. By (6),

$$S_{f\chi,1}(n) = o(n),$$

so for  $n$  sufficiently large, we have

$$(8) \quad |S_{fg,n}(\beta)| \leq \frac{\epsilon n}{m}.$$

To deal with  $\alpha \notin \mathbb{Q}$ , we follow [8, §6]. For each  $\alpha$ , we choose the rational value  $\beta = r/s$  with  $s < n/m$  which is closest to  $\alpha$ . Thus,

$$|\alpha - \beta| \leq \frac{m}{ns}.$$

Summing by parts, we have

$$\begin{aligned} S_{fg,n}(\alpha) &= \sum_{x=1}^n e((\alpha - \beta)x) e(\beta x) f(x) g(x) \\ &= e((\alpha - \beta)n) S_{fg,n}(\beta) + \sum_{y=1}^{n-1} e((\alpha - \beta)y) (1 - e(\alpha - \beta)) S_{fg,y}(\beta). \end{aligned}$$

If  $s \geq m$ , by (7),

$$\begin{aligned} |S_{fg,n}(\alpha)| &\leq |S_{fg,n}(\beta)| + |\alpha - \beta| \sum_{1 \leq y \leq n/m} |S_{fg,y}(\beta)| + |\alpha - \beta| \sum_{n/m < y \leq n} |S_{fg,y}(\beta)| \\ &\leq \epsilon n + \frac{1}{n} \left(\frac{n}{m}\right)^2 + \frac{1}{n} n^2 \epsilon \leq \left(\frac{1}{m^2} + 2\epsilon\right)n. \end{aligned}$$

If  $s < m$ , by (8),

$$\begin{aligned} |S_{fg,n}(\alpha)| &\leq |S_{fg,n}(\beta)| + |\alpha - \beta| \sum_{1 \leq y \leq n/m} |S_{fg,y}(\beta)| + |\alpha - \beta| \sum_{n/m < y \leq n} |S_{fg,y}(\beta)| \\ &\leq \epsilon n + \frac{m}{n} \left(\frac{n}{m}\right)^2 + \frac{m}{n} \frac{n^2 \epsilon}{m} \leq \left(\frac{1}{m} + 2\epsilon\right)n. \end{aligned}$$

Either way, sending  $\epsilon \rightarrow 0$  and  $m \rightarrow \infty$ , we get the lemma.  $\square$

We can now prove Theorem 3.

*Proof.* Applying Lemma 4 with  $D = D_G$ , we may assume  $a, b, c$  satisfy conditions (a)–(f). Given  $\delta > 0$ , let  $T(\delta)$  denote the smallest integer such that

$$\sum_{p \in \mathbb{P}_G \cap [T(\delta), \infty)} \frac{1}{p} < \delta.$$

Let  $\mathfrak{X}$  consist of all integers congruent to 1 (mod  $D$ ) and not divisible by any prime  $p \in \mathbb{P}_G \cap [2, T(\delta)]$ . Let  $\mathfrak{X}'$  denote the set of elements of  $\mathfrak{X}$  divisible by no prime in  $\mathbb{P}_G$ . Let  $X_N := \mathfrak{X} \cap [1, N]$  and  $X'_N := \mathfrak{X}' \cap [1, N]$ . By construction,

$$|(X_N \cap G) \setminus (X'_N \cap G)| \leq |X_N \setminus X'_N| < \delta N$$

for  $N$  sufficiently large. Moreover,

$$f(x) = g(y) = h(z) = 1$$

for all  $f, g, h \in Q_{\text{pre}}^*$  and  $x, y, z \in X'_N$ .

Let  $\Sigma(X)$  denote the number of solutions of  $ax + by + cz = 0$  with  $x, y, z \in X$ . By (3) and (4),  $\Sigma(X_N \cap G)$  is given by

$$(9) \quad |Q|^{-3} \sum_{f, g, h \in Q^*} \int_0^1 \left( \sum_{x \in X_N} f(x) e(axy) \right) \left( \sum_{y \in X_N} g(y) e(byt) \right) \left( \sum_{z \in X_N} h(z) e(czt) \right) dt.$$

By Lemma 6 and Lemma 8, if  $f$  is not pretentious, the summand is  $o(N^2)$ . The same is true if  $g$  or  $h$  is not pretentious.

By construction, for  $f, g, h \in Q_{\text{pre}}^*$ , we have  $f(x) = g(y) = h(z) = 1$  for all  $x, y, z \in X'_N$ , so by (3),

$$\Sigma(X'_N) = \int_0^1 \left( \sum_{x \in X'_N} f(x) e(axy) \right) \left( \sum_{y \in X'_N} g(y) e(byt) \right) \left( \sum_{z \in X'_N} h(z) e(czt) \right) dt.$$

Applying Corollary 7 twice, we have

$$\begin{aligned}
& \left| \int_0^1 \left( \sum_{x \in X_N} f(x)e(axt) \right) \left( \sum_{y \in X_N} g(y)e(byt) \right) \left( \sum_{z \in X_N} h(z)e(czt) \right) dt - \Sigma(X_N) \right| \\
& \leq \left| \int_0^1 \left( \sum_{x \in X_N} f(x)e(axt) \right) \left( \sum_{y \in X_N} g(y)e(byt) \right) \left( \sum_{z \in X_N} h(z)e(czt) \right) dt - \Sigma(X'_N) \right| \\
& \quad + |\Sigma(X'_N) - \Sigma(X_N)| \\
& \leq 6\delta |X_N|^2.
\end{aligned}$$

Combining this with (9), we obtain

$$\left| \Sigma(X_N \cap G) - \frac{|Q_{\text{pre}}^*|^3}{|Q|^3} \Sigma(X_N) \right| = O(\delta N^2).$$

Since  $\sum_{p \in \mathbb{P}_G} p^{-1} < \infty$ , Lemma 5 implies

$$\limsup \frac{\Sigma(X_N)}{N^2} > 0.$$

It follows that by choosing  $\delta$  sufficiently small, we can guarantee

$$\limsup \frac{\Sigma(X_N \cap G)}{N^2} > 0.$$

□

We remark that the method of proof applies equally to the problem of solving the linear equation  $ax + by + cz = 0$  where  $x \in X$ ,  $y \in Y$ , and  $z \in Z$ , where  $X$ ,  $Y$ , and  $Z$  are possibly distinct finite index subgroups of  $\mathbb{Q}^\times$ .

We conclude this section with a proposition showing that the equation (1) with  $x, y, z \in G$  does not satisfy the naive Hasse principle.

**Proposition 9.** *There exists a finite index subgroup  $G$  of  $\mathbb{Q}^\times$  and non-zero  $a, b, c \in \mathbb{Z}$  such that  $ax + by + cz = 0$  has no solution in  $G$  but does have a solution in the completion of  $G$  in  $\mathbb{Q}_v^\times$  for each place  $v$  of  $\mathbb{Q}$ .*

*Proof.* We define

$$G := \{3^m 5^n x \mid m, n \in \mathbb{Z}, m \equiv n \pmod{4}, x \in \mathbb{Q}^\times \cap \mathbb{Z}_3 \cap \mathbb{Z}_5, x \equiv 1 \pmod{15}\}.$$

Thus  $G$  is of index  $4 \cdot \phi(15) = 32$  in  $\mathbb{Q}^\times$ . It is dense in  $\mathbb{Q}_v^\times$  for  $v \notin \{3, 5\}$  and for  $v = p \in \{3, 5\}$  its closure in  $\mathbb{Q}_v^\times$  is

$$G_{\{v\}} = p^{\mathbb{Z}} \{x \in \mathbb{Z}_p^\times \mid x \equiv 1 \pmod{p}\}.$$

However,  $G_{\{3,5\}}$  is not the product  $G_{\{3\}} \times G_{\{5\}}$ ; rather, it is

$$\{(x_3, x_5) \in G_{\{3\}} \times G_{\{5\}} \mid v_3(x_3) \equiv v_5(x_5) \pmod{4}\}.$$

Now, the equation

$$63x + 30y + 25z = 0$$

has solutions in  $G_{\{3\}}$  (for instance  $(-5, 3, 9)$ ), but all such solutions satisfy

$$v_3(x) = v_3(y) - 1 = v_3(z) - 2.$$



It also has solutions in  $G_{\{5\}}$  (for instance  $(25, -45, -9)$ ), but all such solutions satisfy

$$v_5(x) = v_5(y) + 1 = v_5(z) + 2.$$

Therefore, there are no solutions in  $G_{\{3,5\}}$  and, a fortiori, no solutions in  $G$ .  $\square$

### 3. POINTS ON DIAGONAL CURVES

This section gives a proof of Theorem 1. It is easy to see that  $G_K$  finitely generated implies  $K^\times/(K^\times)^n$  finite (see, e.g., [3]). We begin by proving Theorem 2.

*Proof.* Suppose  $ax^n + by^n + cz^n = 0$  has a non-trivial solution  $(\alpha, \beta, \gamma) \in K$ . Replacing  $a, b, c$  by  $a' := a\alpha^n, b' := b\beta^n, c' := c\gamma^n$  respectively, it suffices to prove that the projective curve  $X' : a'x^n + b'y^n + c'z^n = 0$  has infinitely many points in  $K$  such that  $x \neq 0, y \neq 0$ , and  $z \neq 0$ . Since there are only finitely many points of  $X'$  for which any of the coordinates is zero, it suffices to prove  $X'(K)$  is infinite. The advantage of  $X'$  over  $X$  is that  $a' + b' + c' = 0$ . Let  $E \subset K$  be a number field containing  $a', b', c'$ . As  $E$  is infinite, we can find pairwise distinct  $p, q, r \in E^\times$  such that  $a'p + b'q + c'r = 0$  and an infinite sequence  $h_1, h_2, \dots \in E$  such that all finite linear combinations of the  $h_i$  with coefficients in  $\{p, q, r\}$  are distinct from one another. For each positive integer  $k$ , the map  $f_k : \{p, q, r\}^k \rightarrow E$  defined by

$$f_k(x_1, \dots, x_k) = h_1x_1 + \dots + h_kx_k$$

is injective and takes only non-zero values.

Let  $H := (K^\times)^n \cap E^\times$ . Let  $m$  denote the index of  $H$  in  $E^\times$ , which is finite. For every positive integer  $k$  the coset decomposition of  $E^\times$  induces via  $f_k$  a partition of  $\{p, q, r\}^k$  into  $m$  subsets. By the Hales-Jewett theorem, if  $k$  is sufficiently large, there exist  $k$  functions  $g_1, \dots, g_k : \{1, 2, 3\} \rightarrow \{p, q, r\}$  such that for each  $i$ , either  $g_i$  is constant or

$$(g_i(1), g_i(2), g_i(3)) = (p, q, r),$$

and the three terms

$$f_k(g_1(j), \dots, g_k(j)), \quad j = 1, 2, 3,$$

lie in the same part of the partition. If  $I \subset \{1, \dots, k\}$  denotes the set of indices  $i$  for which  $g_i$  is constant, we set

$$A = \sum_{i \in I} g_i(1)h_i, \quad B = \sum_{i \in \{1, \dots, k\} \setminus I} h_i,$$

and then  $A + Bp, A + Bq, A + Br$  all belong to the same part of the partition, i.e., to the same coset of  $H$ . If  $C$  belongs to the inverse coset, then

$$(C(A + Bp), C(A + Bq), C(A + Br)) \in (E^\times)^n \times (E^\times)^n \times (E^\times)^n.$$

Thus,

$$((C(A + Bp))^{1/n}, (C(A + Bq))^{1/n}, (C(A + Br))^{1/n})$$

lies on  $X'(E) \subset X'(K)$ . □

Now we prove Theorem 1.

*Proof.* By Theorem 2 it suffices to prove that  $(1) \Leftrightarrow (2)$ . For  $\mathbb{Q}_v$  any completion of  $\mathbb{Q}$  (i.e.,  $\mathbb{R}$  or  $\mathbb{Q}_p$  for some  $p$ ), we fix an algebraic closure of  $\bar{\mathbb{Q}}_v$ . The algebraic closure  $\mathbb{Q}^{\text{cl},v}$  of  $\mathbb{Q}$  in  $\bar{\mathbb{Q}}_v$  is (non-canonically) isomorphic to  $\bar{\mathbb{Q}}$ . Fixing an isomorphism  $i_v: \bar{\mathbb{Q}} \rightarrow \mathbb{Q}^{\text{cl},v}$ , the restriction map defines an injective homomorphism  $G_{\mathbb{Q}_v} \rightarrow \text{Gal}(\mathbb{Q}^{\text{cl},v}/\mathbb{Q})$  and via  $i_v$  we obtain an injection  $j_v: G_{\mathbb{Q}_v} \rightarrow G_{\mathbb{Q}}$ . As a topological group,  $G_{\mathbb{Q}_v}$  is finitely generated; this is trivial if  $v$  is archimedean and well-known (see, e.g., [1, 5, 6, 11]) in the non-archimedean case. The invariant field  $K_v$  of  $\bar{\mathbb{Q}}$  by  $j_v(G_{\mathbb{Q}_v})$  is isomorphic via  $i_v$  to a subfield of  $\mathbb{Q}_v$ , so (2) implies that  $X(K_v)$ , and therefore  $X(\mathbb{Q}_v)$ , is non-empty.

For the implication  $(1) \Rightarrow (2)$ , we define  $G = \mathbb{Q}^\times \cap (K^\times)^n$ , so  $G$  is of finite index in  $\mathbb{Q}^\times$ . We apply Theorem 3 to  $G$ . In particular,  $G \supset (\mathbb{Q}^\times)^n$ , so by weak approximation, for any finite set  $S$  of places  $v$ , the closure  $G_S$  of  $G$  in  $\mathbb{Q}_S^\times$  contains

$$\prod_{v \in S} (\mathbb{Q}_v^\times)^n.$$

In particular, if  $X(\mathbb{Q}_v)$  has a point  $(x_v : y_v : z_v)$  for each  $v$ , then  $au + bv + cw = 0$  has a solution in  $G_S$  for all  $S$  and therefore in  $\mathbb{Q}$  itself, namely  $u_v = x_v^n, v_v = y_v^n, w_v = z_v^n$ . □

**Corollary 10.** *If  $X$  is a diagonal curve, then  $X(K)$  is infinite for all  $K \subset \bar{\mathbb{Q}}$  with  $G_K$  finitely generated if and only if  $X(\mathbb{A}_{\mathbb{Q}}) \neq \emptyset$ , where  $\mathbb{A}_{\mathbb{Q}}$  denotes the ring of adeles.*

*Proof.* The only additional point to check is that for any  $a, b, c \in \mathbb{Q}^\times$ , there exists a finite set  $S$  of places of  $\mathbb{Q}$ , including  $\infty$ , such that  $X$  has a point over  $\mathbb{Z}_p$  for all  $p \notin S$ . If  $p$  is sufficiently large,  $a, b$ , and  $c$  are  $p$ -adic units, so  $X$  has good reduction (mod  $p$ ), and the reduction is a curve of genus  $\frac{(n-1)(n-2)}{2}$ . If  $p > (n-1)^2(n-2)^2$ , the Weil bound implies that  $X$  has at least one points over  $\mathbb{F}_p$ , and Hensel's lemma implies that any such point lifts to a  $\mathbb{Z}_p$ -point. □

**Question 11.** *Is it always true that for  $X$  a non-singular curve over a number field  $E$ , there exists an  $\mathbb{A}_E$ -point on  $X$  if and only if for all  $K \subset \bar{\mathbb{Q}}$  with  $G_K$  finitely generated,  $X(K)$  is infinite?*

The circle method offers the hope of giving an affirmative answer to this question for some non-diagonal curves. We hope to treat this matter in a subsequent paper.

## REFERENCES

- [1] Diekert, Volker: Über die absolute Galoisgruppe dyadischer Zahlkörper. *J. Reine Angew. Math.* **350** (1984), 152–172.

- [2] Granville, Andrew; Soundararajan, K.: Large character sums: pretentious characters and the Pólya-Vinogradov theorem. *J. Amer. Math. Soc.* **20** (2007), no. 2, 357–384.
- [3] Im, Bo-Hae; Larsen, Michael: Generalizing a theorem of Richard Brauer. *J. Number Theory* **128** (2008), no. 12, 3031–3036.
- [4] Im, Bo-Hae; Larsen, Michael: Some applications of the Hales-Jewett theorem to field arithmetic. *Israel J. Math.* **198** (2013), no. 1, 35–47.
- [5] Jannsen, Uwe: Über Galoisgruppen lokaler Körper. *Invent. Math.* **70** (1982/83), no. 1, 53–69.
- [6] Jannsen, Uwe; Wingberg, Kay: Die Struktur der absoluten Galoisgruppe  $p$ -adischer Zahlkörper. *Invent. Math.* **70** (1982/83), no. 1, 71–98.
- [7] Knapp, Anthony W.: Elliptic curves. Mathematical Notes, 40. Princeton University Press, Princeton, NJ, 1992.
- [8] Montgomery, H. L.; Vaughan, R. C.: Exponential sums with multiplicative coefficients. *Invent. Math.* **43** (1977), no. 1, 69–82.
- [9] Rado, Richard: Studien zur Kombinatorik. *Math. Z.* **36** (1933), no. 1, 424–470.
- [10] Tenenbaum, Gérald: Introduction to analytic and probabilistic number theory. Cambridge Studies in Advanced Mathematics, 46. Cambridge University Press, Cambridge, 1995.
- [11] Wingberg, Kay: Der Eindeutigkeitsatz für Demuškinformationen. *Invent. Math.* **70** (1982/83), no. 1, 99–113.

SCHOOL OF MATHEMATICS, INSTITUTE FOR ADVANCED STUDY, EINSTEIN DRIVE,  
PRINCETON, NJ 08540, USA

*E-mail address:* bourgain@math.ias.edu

DEPARTMENT OF MATHEMATICS, INDIANA UNIVERSITY, BLOOMINGTON, INDIANA 47405,  
USA

*E-mail address:* mjlarsen@indiana.edu